PCT/JP00/00658
07.02.00

EJU

# 日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 18 FEB 2000
WIPO PCT

JP00/658

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年 ２月 ８日

出願番号
Application Number: 平成１１年特許願第０３０６００号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年１２月２４日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特平１１－３０９１１８０

【書類名】　特許願

【整理番号】　9900070509

【提出日】　平成11年 2月 8日

【あて先】　特許庁長官　殿

【国際特許分類】　G11B　7/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　大澤　義知

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100067736

【弁理士】

【氏名又は名称】　小池　晃

【選任した代理人】

【識別番号】　100086335

【弁理士】

【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録／再生システム、情報記録装置、情報再生装置、認証データ記録装置、情報記録媒体、認証データの記録方法、情報記録媒体の認証方法、情報記録方法及び情報再生方法

【特許請求の範囲】

【請求項１】　情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録装置と、

上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行い、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体を介して記録／再生する情報記録／再生装置と

からなる情報記録／再生システム。

【請求項２】　上記認証データ記録装置は、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することを特徴とする請求項１記載の情報記録／再生システム。

【請求項３】　上記情報記録／再生装置は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記ユーザデータの暗号化に用いる暗号鍵を暗号化し、上記暗号鍵により暗号化したユーザデータと上記暗号化した暗号鍵を上記認証された情報記録媒体を介して記録／再生することを特徴とする請求項１記載の情報記録／再生システム。

【請求項４】　上記情報記録／再生装置は、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、上記ユーザデータの暗号化に用いる暗号鍵を生成することを特徴とする請求項３記載の情報記録／再生システム。

【請求項５】　ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体にユーザデータを記録する情報記録装置であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、

上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、

情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、

上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、上記暗号鍵と暗号化したユーザデータを上記認証された情報記録媒体に記録する記録手段と

を備えることを特徴とする情報記録装置。

【請求項６】　上記認証処理手段は、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項５記載の情報記録装置。

【請求項７】　上記認証処理手段は、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求

項５記載の情報記録装置。

【請求項８】　上記認証処理手段は、上記リボケーションリストを格納する記憶手段を有し、情報記録媒体に記録されていたリボケーションリストが正当なものであり、上記記憶手段に格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを上記記憶手段に格納し、上記記憶手段に格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項７記載の情報記録装置。

【請求項９】　上記記録手段は、暗号鍵を生成する暗号鍵生成手段と、上記媒体識別情報を用いて上記暗号鍵を暗号化する暗号鍵暗号化手段と、上記暗号鍵を用いてユーザデータを暗号化するユーザデータ暗号化手段とを備え、

上記ユーザデータ暗号化手段により暗号化したユーザデータと上記暗号鍵暗号化手段により暗号化した暗号鍵を上記認証された情報記録媒体に記録することを特徴とする請求項５記載の情報記録装置。

【請求項１０】　上記暗号鍵生成手段は、上記媒体識別情報を用いて暗号鍵を生成することを特徴とする請求項９記載の情報記録装置。

【請求項１１】　ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体からユーザデータを再生する情報再生装置であって、

情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、

上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、

情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、

上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて暗号

鍵を生成する暗号鍵生成手段と、

上記暗号鍵生成手段により生成された暗号鍵を用いてユーザデータを復号する復号手段を備え、

上記認証処理手段により認証された情報記録媒体上のユーザデータ記録部から、上記媒体識別情報を用いて生成された暗号鍵により暗号化されたユーザデータを上記復号手段により復号して再生することを特徴とする情報再生装置。

【請求項１２】　上記認証処理手段は、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと検証された正当な媒体識別情報に基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項１１記載の情報再生装置。

【請求項１３】　上記認証処理手段は、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項１２記載の情報再生装置。

【請求項１４】　上記認証処理手段は、上記リボケーションリストを格納する記憶手段を有し、情報記録媒体に記録されていたリボケーションリストが正当なものであり、上記記憶手段に格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを上記記憶手段に格納し、上記記憶手段に格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項１１記載の情報再生装置。

【請求項１５】　ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出手段と、

上記ランダムパターン情報検出手段により検出された上記ランダムパターン情

報から媒体識別情報を生成する媒体識別情報生成手段と、

上記媒体識別情報生成手段により生成した媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録手段と

を備えることを特徴とする認証データ記録装置。

【請求項１６】　上記認証データ記録手段は、上記認証データ記録部に製造者についてのリボケーションリストを上記認証データとともに記録することを特徴とする請求項１５記載の認証データ記録装置。

【請求項１７】　ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部と、

上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部と、

ユーザデータが記録されるユーザデータ記録部と

を有することを特徴とする情報記録媒体。

【請求項１８】　上記認証データ記録部に製造者についてのリボケーションリストが上記認証データとともに記録されたことを特徴とする請求項１７記載の情報記録媒体。

【請求項１９】　情報記録媒体に記録されたランダムな物理現象によるランダムパターン情報を検出し、

上記ランダムパターン情報から媒体識別情報を生成し、

上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体に記録する

ことを特徴とする認証データの記録方法。

【請求項２０】　製造者についてのリボケーションリストを上記認証データとともに上記情報記録媒体に記録することを特徴とする請求項１９記載の認証データの記録方法。

【請求項２１】　情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が該媒体識別情報に対する製造者

毎のデジタル署名とともに認証データとして記録された情報記録媒体から、

上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、

上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて、上記情報記録媒体の認証処理を行う

ことを特徴とする情報記録媒体の認証方法。

【請求項２２】　製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、

上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、正当なデジタル署名に基づいて認証処理を行う

ことを特徴とする請求項２１記載の情報記録媒体の認証方法。

【請求項２３】　製造者についてのリボケーションリストを記憶しておき、

情報記録媒体に記録されていたリボケーションリストが正当なものであり、先に記憶したリボケーションリストよりも新しい場合に、記憶していたリボケーションリストを更新し、

最新のリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項２１記載の情報記録媒体の認証方法。

【請求項２４】　扱った情報記録媒体の製造者の識別情報とその公開鍵をリボケーションフラグとともに記憶して記憶しておき、新しいリボケーションリストを用いてリボケーションフラグを更新し、

リボケーションフラグを用いて上記認証データに含まれるデジタル署名の正当性を検証し、正当なデジタル署名に基づいて認証処理を行う

ことを特徴とする請求項２１記載の情報記録媒体の認証方法。

【請求項２５】　情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、

上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情

報検査データを生成するとともに、

上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、

上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、

上記暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体に記録することを特徴とする情報記録方法。

【請求項２６】　暗号鍵によりユーザデータを暗号化するとともに、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて上記暗号鍵を暗号化し、

上記暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体に記録することを特徴とする請求項２５記載の情報記録方法。

【請求項２７】　上記媒体識別情報を用いて暗号鍵を生成し、上記暗号鍵によりユーザデータを暗号化することを特徴とする請求項２６記載の情報記録方法。

【請求項２８】　上記認証処理では、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、検証された正当な媒体識別情報と上記媒体識別情報検査データに基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項２５記載の情報記録方法。

【請求項２９】　上記認証処理では、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項２５記載の情報記録方法。

【請求項３０】　上記認証処理では、情報記録媒体に記録されていたリボケーションリストが正当なものであり、格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを新た

に格納し、格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項２９記載の情報記録方法。

【請求項３１】　情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、

上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、

上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、

認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、

上記暗号鍵を用いてユーザデータを復号し、

上記認証された情報記録媒体から上記暗号鍵を用いてユーザデータを復号することを特徴とする情報再生方法。

【請求項３２】　上記認証処理では、上記媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体に対し、上記製造者毎のデジタル署名に基づいて上記媒体識別情報の正当性を検証し、検証された正当な媒体識別情報と上記媒体識別情報検査データに基づいて情報記録媒体に対する認証処理を行うことを特徴とする請求項３１記載の情報再生方法。

【請求項３３】　上記認証処理では、製造者についてのリボケーションリストが上記認証データとともに記録された情報記録媒体に対し、上記リボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項３１記載の情報再生方法。

【請求項３４】　上記認証処理では、情報記録媒体に記録されていたリボケーションリストが正当なものであり、格納されているリボケーションリストよりも新しい場合に、上記情報記録媒体に記録されていたリボケーションリストを新た

に格納し、格納したリボケーションリストに基づいて、上記認証データに含まれるデジタル署名の正当性を検証し、検証された正当なデジタル署名に基づいて認証処理を行うことを特徴とする請求項３３記載の情報再生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＲＡＭメディアに対する不正コピーを防止するようにした情報記録／再生システム、情報記録装置、情報再生装置、認証データ記録装置、情報記録媒体、認証データの記録方法、情報記録媒体の認証方法、情報記録方法及び情報再生方法に関する。

【０００２】

【従来の技術】

近年、家庭内において音楽情報や映像情報などのデジタルデータを伝送したり記録したりする機器が広く普及している。これらの機器では、データを高品質で記録／再生することが可能であることから、何度複製しても品質劣化のない記録システムを構成することができる。このような記録システムでは、著作権のあるデータが不正にコピーされてしまうのを防止する著作権保護機能を装備する必要がある。

【０００３】

このような著作権保護のためのシステムとして、例えば、Digital Video Disc (DVD) ROM におけるコンテンツスクランブルシステムがある。

【０００４】

このシステムでは、ディスク上の著作権付きデータをすべて暗号化し、ライセンスを受けた機器だけが、暗号を復号して意味のあるデータを得るための暗号鍵を与えられるようにしている。ライセンスを受けた機器は、不正コピーを行わないなどの動作規定に従うように設計されている。

【０００５】

【発明が解決しようとする課題】

しかし、上述の如きＤＶＤシステムが採用している方式は、ＲＯＭメディアに

対して有効であるが、ユーザがデータを記録可能なＲＡＭメディアにおいては有効でない。なぜならば、ＲＡＭメディアにおいては、不正者は、暗号を解読できないとしても、ディスク上のデータを全部、新しいディスクにコピーすることによって、正当な機器では動作してしまうディスクを新たに作ることができるからである。

【０００６】

そこで、本発明の目的は、ＲＡＭメディアに対しても有効な不正コピー防止システムを構築した情報記録／再生システム、情報記録装置、情報再生装置、認証データ記録装置、情報記録媒体、認証データの記録方法、情報記録媒体の認証方法、情報記録方法及び情報再生方法を提供することにある。

【０００７】

【課題を解決するための手段】

本発明に係る情報記録／再生システムは、情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録装置と、上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて上記情報記録媒体に対する認証処理を行い、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体を介して記録／再生する情報記録／再生装置とからなる。

【０００８】

本発明に係る情報記録装置は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部

から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体にユーザデータを記録する情報記録装置であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、上記暗号鍵と暗号化したユーザデータを上記認証された情報記録媒体に記録する記録手段とを備えることを特徴とする。

【０００９】

本発明に係る情報再生装置は、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報を認証データとして格納した認証データ記録部とを有する情報記録媒体からユーザデータを再生する情報再生装置であって、情報記録媒体上のランダムパターン情報記録部からランダムパターン情報を検出するランダムパターン情報検出手段と、上記ランダムパターン情報検出手段により検出されたランダムパターン情報から媒体識別情報検査データを生成する媒体識別情報検査データ生成手段と、情報記録媒体上の認証データ記録部から認証データを再生し、上記媒体識別情報検査データ生成手段により生成された媒体識別情報検査データと上記認証データに基づいて情報記録媒体に対する認証処理を行う認証処理手段と、上記認証処理手段により認証された情報記録媒体の媒体識別情報を用いて暗号鍵を生成する暗号鍵生成手段と、上記暗号鍵生成手段により生成された暗号鍵を用いてユーザデータを復号する復号手段を備え、上記認証処理手段により認証された情報記録媒体上のユーザデータ記録部から、上記媒体識別情報を用いて生成された暗号鍵により暗号化されたユーザデータを上記復号手段により復号して再生することを特徴とする

【００１０】

本発明に係る認証データ記録装置は、ランダムな物理現象によるランダムパターン情報が記録された情報記録媒体上のランダムパターン情報記録部から上記ランダムパターン情報を検出するランダムパターン情報検出手段と、上記ランダムパターン情報検出手段により検出された上記ランダムパターン情報から媒体識別情報を生成する媒体識別情報生成手段と、上記媒体識別情報生成手段により生成した媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証データとして上記情報記録媒体上の認証データ記録部に記録する認証データ記録手段とを備えることを特徴とする。

【００１１】

本発明に係る情報記録媒体は、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部と、ユーザデータが記録されるユーザデータ記録部とを有することを特徴とする。

【００１２】

本発明に係る認証データの記録方法は、情報記録媒体に記録されたランダムな物理現象によるランダムパターン情報を検出し、上記ランダムパターン情報から媒体識別情報を生成し、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体に記録することを特徴とする。

【００１３】

本発明に係る情報記録媒体の認証方法は、情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして記録された情報記録媒体から、上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記認証データを再生し、

上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて、上記情報記録媒体の認証処理を行うことを特徴とする。

【００１４】

本発明に係る情報記録方法は、情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、上記認証処理により認証された情報記録媒体の媒体識別情報を用いて、暗号鍵とユーザデータの暗号化に関わる処理を行い、上記暗号化したユーザデータと暗号鍵を上記認証された情報記録媒体に記録することを特徴とする。

【００１５】

本発明に係る情報再生方法は、情報記録媒体上に記録されたランダムな物理現象によるランダムパターン情報から生成された媒体識別情報が認証データとして記録された情報記録媒体に対し、上記ランダムパターン情報を検出して該ランダムパターン情報から媒体識別情報検査データを生成するとともに、上記認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報検査データと上記認証データに基づいて認証処理を行い、認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてユーザデータを復号し、上記認証された情報記録媒体から上記暗号鍵を用いてユーザデータを復号することを特徴とする。

【００１６】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【００１７】

本発明は、例えば図１に示すような構成の光ディスク１を用いた記録／再生システムに適用される。

【００１８】

図１に示した光ディスク１は、情報の記録／再生可能なＲＡＭディスクであり、中心孔２を中心としてそれぞれ環状に形成された３つの情報記録領域であるユーザデータ記録部３、ランダムパターン情報記録部４及び認証データ記録部５を有する。上記ユーザデータ記録部３、ランダムパターン情報記録部４及び認証データ記録部５は、それぞれ独立にアクセスして情報を読み出すことができるように、例えば、２次元的に分離した状態、又は、３次元的に分離した状態に配置される。

【００１９】

この光ディスク１では、情報記録領域をディスク半径方向に２次元的に分離することにより、上記ユーザデータ記録部３、ランダムパターン情報記録部４及び認証データ記録部５が形成されている。

【００２０】

この光ディスク１において、外周側に形成されたユーザデータ記録部３は、ユーザデータが記録／再生されるデータエリアである。

【００２１】

また、内周側に形成されたランダムパターン情報記録部４は、ランダムな物理現象によるランダムパターン情報が記録された読み取り専用の領域である。

【００２２】

このランダムパターン情報記録部４は、メディアの製造時に例えば磁気を帯びた細かい繊維を、このランダムパターン情報記録部４の領域にランダムに撒いて固定するすることにより形成される。このようにして形成されたランダムパターン情報記録部４は、上記磁気を帯びた細かい繊維によるランダムパターン情報が検出可能に記録されたものとなる。

【００２３】

なお、上記ランダムパターン情報記録部４は、ランダムにビットを形成し、そのジッターをランダムパターン情報として検出するできるようにしてもよい。

【００２４】

さらに、上記ランダムパターン情報記録部４の外周側に形成された認証データ

記録部５は、上記ランダムパターン情報記録部４から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された領域である。この認証データ記録部５は、リードインエリアに設けられている。

【００２５】

このような構成の光ディスク１は、例えば図２に示すような構成の認証データ記録装置１０により、上記認証データ記録部５に認証データが記録される。

【００２６】

この図２に示した認証データ記録装置１０は、サーボ回路１１により制御されるスピンドルモータ１２、上記光ディスク１の情報記録面を光学的に走査する記録／再生ヘッド１３、上記光ディスク１のランダムパターン情報記録部４からランダムパターン情報を検出するランダムパターン情報検出部１４、媒体識別情報ｒを生成する媒体識別情報生成部１５、 認証データを生成する認証データ生成部１６、入力操作部１７から入力される設定情報に基づいて上記サーボ回路１１や認証データ生成部１６を制御する制御部１８等を備える。

【００２７】

上記スピンドルモータ１２は、サーボ回路１１による制御に基づいて、上記光ディスク１を例えば線速度一定の状態で回転駆動させる。

【００２８】

上記記録／再生ヘッド１３は、上記スピンドルモータ１２により回転駆動される光ディスク１の認証データ記録部５を光学的に走査する光学ヘッドからなり、上記認証データ記録部５を介して認証データの記録／再生を行う。

【００２９】

上記ランダムパターン情報検出部１４は、上記スピンドルモータ１２により回転駆動される光ディスク１のランダムパターン情報記録部４を走査する磁気ヘッドからなり、上記ランダムパターン情報記録部４からランダムパターン情報をアナログ的に検出する。このランダムパターン情報検出部１４は、上記ランダムパターン情報記録部４から検出したランダムパターン情報を上記媒体識別情報生成部１５に供給する。

【００３０】

上記媒体識別情報生成部１５は、上記ランダムパターン情報検出部１４によりアナログ的に検出されたランダムパターン情報からデジタルのランダムパターン情報に変換し、これを媒体識別情報ｒとして上記認証データ生成部１６に供給する。

【００３１】

上記認証データ生成部１６は、上記媒体識別情報生成部１５から供給される媒体識別情報ｒに該媒体識別情報ｒに対する製造者毎のデジタル署名を付して認証データとする。

【００３２】

ここで、上記認証データ生成部１６により製造者毎のデジタル署名を付した認証データを生成するに当たり、記録媒体の製造者は、信頼できるトラステッド・センター(TC:Trasted Center) を使用し、デジタル署名の検証に必要な自分の公開鍵をＴＣに登録し、証明書(Cert)を発行してもらっておく。証明書(Cert)は、製造者の識別情報ＩＤや公開鍵などにＴＣがデジタル署名を施したデータである。

【００３３】

また、デジタル署名技術は、あるデータを生成したのがあるユーザであることを証明できる技術であり、例えばＩＥＥＥ　Ｐ１３６３で使用されているElliptic Curve Digital Signature Algorithm(EC-DSA)方式などがよく知られている。

【００３４】

この認証データ記録装置１０では、上記認証データ生成部１６の具体的な処理内容を図３に示してあるように、上記媒体識別情報生成部１５から供給される媒体識別情報ｒに媒体製造日や製造者番号などの付加情報ｕを付加して、データｍを生成する（ステップＳ１）。このデータｍに対し、トラステッド・センターに登録した公開鍵に対応する製造者別の秘密鍵を用いてデジタル署名データｓを生成する（ステップＳ２）。

【００３５】

なお、上記付加情報ｕは、必要に応じて上記媒体識別情報ｒに付加すればよい

データである。

【００３６】

そして、上記認証データ生成部１６は、上記データｍとデジタル署名データｓと証明書(Cert)データをリボケーションリストを合わせて認証データｗとし（ステップＳ３）、この認証データｗを上記記録／再生ヘッド１３に供給する（ステップＳ４）ことにより、上記光ディスク１の認証データ記録部５に記録する。

【００３７】

ここで、上記付加情報ｕ、製造者別の秘密鍵及び証明書(Cert)データは、例えば上記入力操作部１７から上記制御部１８に入力されることにより、上記制御部１８から上記認証データ生成部１６に与えられる。

【００３８】

この認証データ記録装置１０では、トラステッド・センターから与えられるリボケーションリストを上記入力操作部１７から上記制御部１８に入力することにより、上記リボケーションリストを上記制御部１８から上記認証データ生成部１６に与えて、上記光ディスク１の認証データ記録部５に記録することができるようになっている。上記光ディスク１の認証データ記録部５には、トラステッド・センターから与えられる最新版のリボケーションリストを記録する。

【００３９】

ここで、リボケーションリストは、単調増加であるそのバージョンナンバーと、秘密鍵が露呈したり不正を働いた判断された製造者の識別情報ＩＤにトラステッド・センターがデジタル署名を施したものである。

【００４０】

記録媒体の製造者は、このような構成の認証データ記録装置１０により、上記データｍとデジタル署名データｓと証明書(Cert)データとリボケーションリストを認証データｗとして認証データ記録部５に記録した光ディスク１を製造することができる。

【００４１】

このような構成の光ディスク１は、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部４から検出されるランダムパタ

ーン情報と、認証データ記録部１６に記録されている認証データによる認証処理により正当性を検証することができる。上記ランダムパターン情報記録部４に記録されているランダムパターン情報は、ランダムな物理現象によるものであるから、複製することはできない。

【００４２】

上述の如き構成の光ディスク１は、例えば図４に示すような構成の光ディスク記録／再生装置２０により、データの記録／再生が行われる。

【００４３】

図４に示した光ディスク記録／再生装置２０は、サーボ回路２１により制御されるスピンドルモータ２２、上記光ディスク１の情報記録面を光学的に走査する記録／再生ヘッド２３、上記光ディスク１のランダムパターン情報記録部４からランダムパターン情報を検出するランダムパターン情報検出部２４、媒体識別情報検査データｒ’を生成する媒体識別情報検査データ生成部２５、 認証処理部２６、記録／再生部２７、入力操作部２８から入力される設定情報に基づいて上記サーボ回路２１や記録／再生部２７を制御する制御部１９等を備える。

【００４４】

上記スピンドルモータ２２は、サーボ回路２１による制御に基づいて、上記光ディスク１を例えば線速度一定の状態で回転駆動させる。

【００４５】

上記記録／再生ヘッド２３は、上記スピンドルモータ２２により回転駆動される光ディスク１の情報記録面を認証データ記録部５を光学的に走査する光学ヘッドからなり、上記認証データ記録部５に記録されている認証データの再生や、上記ユーザデータ部３に対するデータの記録／再生を行う。

【００４６】

上記ランダムパターン情報検出部２４は、上記スピンドルモータ２２により回転駆動される光ディスク１のランダムパターン情報記録部４を走査する磁気ヘッドからなり、上記ランダムパターン情報記録部４からランダムパターン情報をアナログ的に検出する。このランダムパターン情報検出部２４は、上記ランダムパターン情報記録部４から検出したランダムパターン情報を上記媒体識別情報検査

データ生成部２５に供給する。

【００４７】

上記媒体識別情報検査データ生成部２５は、上記ランダムパターン情報検出部２４によりアナログ的に検出されたランダムパターン情報からデジタルのランダムパターン情報に変換し、これを媒体識別情報検査データｒ’として上記認証処理部２６に供給する。

【００４８】

上記認証処理部２６は、上記光ディスク１が正当な製造者により製造されたものであることを認証する処理を行うものである。この認証処理部２６は、上記記録／再生ヘッド２３により上記光ディスク１の認証データ記録部５から再生される認証データｗ＾が記録／再生部２７を介して供給されており、上記媒体識別情報生成部２５から供給される媒体識別情報検査データｒ’と上記認証データｗ＾に基づいて認証処理を行う。

【００４９】

上記認証処理部２６の具体的な処理内容を図５に示してある。

【００５０】

すなわち、上記認証処理部２６は、上記媒体識別情報検査データｒ’と上記認証データｗ＾を取り込むと（ステップＳ１１）、先ず、上記認証データｗ＾に入っているリボケーションリストの正当性すなわちトラステッド・センターのデジタル署名の正当性をトラステッド・センターの公開鍵を用いて検証する（ステップＳ１２）。トラステッド・センターの公開鍵は、システム全体で共通であり、機器を製造する際に機器内の不揮発性メモリに格納されている。

【００５１】

上記リボケーションリストの検証の結果、リボケーションリストが正当なものであったら、上記リボケーションリストのバージョンナンバーを検証し（ステップＳ１３）、現在保存しているリボケーションリストと比較しバージョンナンバーが新しい場合には、不揮発性メモリに格納する（ステップＳ１４）。不揮発性メモリは、図６に示すようなリボケーションリストが格納される。

【００５２】

次に、上記認証データｗ＾中の証明書(Cert)データを取り出し（ステップＳ１５）、上記証明書(Cert)データに含まれる製造者の識別情報ＩＤが上記不揮発性メモリに格納しているリボケーションリストに載っていないことを検証し（ステップＳ１６）、さらに、上記証明書(Cert)データに含まれるトラステッド・センターのデジタル署名が正しいことを検証する（ステップＳ１７）。

【００５３】

この検証に合格したら、上記認証データｗ＾からデータｍ＾とデジタル署名データｓ＾を取り出し（ステップＳ１８）、上記認証データｗ＾中のデジタル署名データｓ＾がデータｍ＾に対する製造者の正しいデジタル署名になっていることを、上記証明書(Cert)データ中の製造者の公開鍵を用いて検証する（ステップＳ１９）。

【００５４】

上記検証に合格したら、検証結果Ｊ２を合格とする（ステップＳ２０）。

【００５５】

次に、上記認証データｗ＾から媒体識別情報ｒ＾と付加情報ｕ＾を取り出す（ステップＳ２１）。

【００５６】

そして、上記認証データｗ＾から取り出した媒体識別情報ｒ＾と上記媒体識別情報生成部２５により生成された媒体識別情報検査データｒ’とを比較し、予め定められた誤差内に収まっていることを検証する（ステップＳ２２）。

【００５７】

この検証に合格したら、検証結果Ｊ１を合格とする（ステップＳ２３）。

【００５８】

上記検証結果Ｊ１と検証結果Ｊ２が共に合格となれば、この記録媒体を正当なものと判断し、上記媒体識別情報ｒ＾を認証済みの媒体識別情報DiscIDとして記録／再生部２７に供給する（ステップＳ２４）。

【００５９】

ここで、上記不揮発性メモリは、図７に示すような公開鍵リストを格納するよ

うにすることもできる。

【００６０】

この場合、公開鍵リストには、製造者の識別情報ＩＤと、その公開鍵、識別情報ＩＤがリボークされているか否かを示すフラグが格納される。さらに、その機器が扱ったことのあるリボケーションリストのうち最新のバージョンのもののバージョンナンバーが格納される。

【００６１】

この機器がデータｗ＾から、機器が扱ったいずれのものより新しい、正当なリボケーションリストを得た場合、そのリストに挙げられている識別情報ＩＤに対応するリボケーションフラグをＹＥＳすなわちリボークとする。

【００６２】

もしそれまでその識別情報ＩＤがテーブル上になければ、その項目を新規に作成してフラグをＹＥＳとする。

【００６３】

逆に、機器が格納していたテーブルにはあったが、最新のリボケーションリストに識別情報ＩＤが含まれていないものについては、フラグをすべてＮＯすなわちリボークしないとする。そして、最新のバージョンナンバーの項目を更新する。

【００６４】

上記認証データｗ＾中から取り出した証明書(Cert)データを検証する際には、製造者の識別情報ＩＤをチェックし、その識別情報ＩＤの項目が格納してあるリストにあり、その公開鍵が記録されていて、リボケーションフラグがＮＯであれば、証明書(Cert)データの検証は不要であり、テーブルに記録されている公開鍵を使用する。

【００６５】

識別情報ＩＤの項目がテーブルにあり、フラグがＮＯであり、公開鍵が記録されていない場合には、証明書(Cert)データを検証して、正しい場合に公開鍵をテーブルに格納する。

【００６６】

識別情報ＩＤの項目がテーブルにあり、フラグがＹＥＳである場合には、検証Ｊ１の結果を不合格とする。

【００６７】

識別情報ＩＤの項目がテーブルにない場合には、証明書(Cert)データを検証して、正しい場合に、その識別情報ＩＤに対応する項目を新規に作成して公開鍵を格納する。このときフラグはＮＯとする。

【００６８】

このように公開鍵リストを持つことにより、多くの場合、すなわち、同一の製造者が製造した媒体を使用するが２回目以降になる場合のほとんどで証明書(Cert)データの検証を省くことが可能となる。

【００６９】

この光ディスク記録／再生装置２０において、上記記録／再生部２７は、入力操作部２８から入力される制御命令に応じて制御部２９により動作モードが切り換えられる。この記録／再生部２７は、暗号化処理部３０と復号処理部４０を備えており、記録モードには、外部から入力されるユーザデータを上記暗号化処理部３０により暗号化し、暗号化したユーザデータを上記記録／再生ヘッド２３を介して上記光ディスク１のユーザデータ部３に記録し、また、再生モード時には、上記記録／再生ヘッド２３により上記光ディスク１のユーザデータ部３から再生される暗号化されたユーザデータを復号処理部４０により復号して外部に出力するようになっている。

【００７０】

上記暗号化処理部３０は、その具体的な構成を図８に示すように、Ｋｅｍ発生モジュール３１、乱数発生回路３２、Ｋｄ暗号化／復号回路３３、Ｋｓ暗号化回路３５やコンテンツデータ暗号化回路３６等からなる。

【００７１】

上記Ｋｅｍ発生モジュール３１は、マスターキーＫｍを記憶したＫｍメモリ３１Ａと、上記Ｋｍメモリ３１Ａから上記マスターキーＫｍが与えられるとともに上記認証処理部２６から認証済みの媒体識別情報DiscIDが供給されるハッシュ関

数回路３１Ｂとからなる。

【００７２】

上記マスターキーＫｍは、著作権のライセンスを受ける際に与えられる秘密鍵である。

【００７３】

上記ハッシュ関数回路３１Ｂは、ｎビットのマスターキーＫｍとｍビットの媒体識別情報DiscIDとを連結して、例えば下位ビットをマスターキーＫｍとし上位ビットを媒体識別情報DiscIDとしたｎ＋ｍビットの連結データ(DiscID‖Ｋｍ)を生成し、生成した連結データ(DiscID‖Ｋｍ)に対して、次の（１）式に示すようにｈａｓｈ関数Ｈを適用して、

Ｋｅｍ＝Ｈ（DiscID‖Ｋｍ）

イフェクティブマスターキーＫｅｍを生成する。そして、上記ハッシュ関数回路３１Ｂは、上記マスターキーＫｍと認証済みの媒体識別情報DiscIDから生成したイフェクティブマスターキーＫｅｍをＫｄ暗号化／復号回路３３に供給する。

【００７４】

ここで、Ａ‖Ｂの‖は、データＡとデータＢの連結を意味する。また、ｈａｓｈ関数は、任意長の入力データに対して、例えば６４ビット又は１２８ビットなどの固定長のデータを出力する関数であり、ｙ（＝ｈａｓｈ(ｘ)）を与えられたとき、ｘを求めることが困難であり、かつ、ｈａｓｈ(ｘ１)＝ｈａｓｈ(ｘ２)となるｘ１とｘ２との組を求めることも困難となる関数である。一方向ｈａｓｈ関数の代表的なものとしてＭＤ(Message Digest)５やＳＨＡ(Soecure Hash Algorithm)などが知られている。この一方向ｈａｓｈ関数については、Bruce Schneier著「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。

【００７５】

また、上記乱数発生回路３２は、乱数をセクタキーＫｓｉとディスクキーＫｄとして用いる乱数を発生し、セクタキーＫｓｉを上記Ｋｓ暗号化回路３５とコンテンツデータ暗号化回路３６に供給するとともに、ディスクキーＫｄを上記Ｋｄ暗号化／復号回路３３とＫｓ暗号化回路３５に供給する。

【００７６】

上記Ｋｄ暗号化／復号回路３３は、上記乱数発生回路３２から供給されるディスクキーＫｄを上記イフェクティブマスターキーＫｅｍで暗号化して暗号化ディスクキーＥＫｄを生成する。このＫｄ暗号化／復号回路３３により生成された暗号化ディスクキーＥＫｄは、上記記録／再生ヘッド２３を介して上記光ディスク１のリードインエリアに記録される。また、このＫｄ暗号化／復号回路３３は、上記記録／再生ヘッド２３を介して上記光ディスク１のリードインエリアから再生される暗号化ディスクキーＥＫｄを復号してディスクキーＫｄを生成する。このＫｄ暗号化／復号回路３３により生成されたディスクキーＫｄは、上記Ｋｓ暗号化回路３５に供給される。

【００７７】

また、上記Ｋｓ暗号化回路３５は、上記乱数発生回路３２から供給されるセクタキーＫｓｉを上記ディスクキーＫｄで暗号化して暗号化セクタキーＥＫｓを生成する。このＫｓ暗号化回路３５により生成された暗号化セクタキーＥＫｓは、上記記録／再生ヘッド２３を介して上記光ディスク１のデータエリアに記録される。

【００７８】

さらに、上記コンテンツデータ暗号化回路３６は、外部からコンテンツデータとして供給されるユーザデータを上記セクタキーＫｓｉで暗号化することにより、暗号化コンテンツデータを生成する。

【００７９】

この上記コンテンツデータ暗号化回路３６により生成された暗号化コンテンツデータは、上記記録／再生ヘッド２３を介して上記光ディスク１のデータエリアに記録される。

【００８０】

ここで、上記光ディスク１のデータエリアは、図９に示すように、複数のセクタＳｉ（ｉ＝１，２，・・・）からなる。各セクタＳｉ（ｉ＝１，２，・・・）は、ヘッダ及びメインデータ部で構成されており、上記セクタキーＫｓｉをディスクキーＫｄで暗号化した暗号化セクタキーＥＫｓｉ（ｉ＝１，２，・・・）が

ヘッダに格納され、ユーザデータを上記セクタキーＫｓｉで暗号化した暗号化コンテンツデータがメインデータ部に格納される。上記ｉ＝１，２，・・・はセクタの番号を示している。なお、簡略化のため、一部の図及び説明文中では、セクタ番号を省略する。

【００８１】

また、上記復号処理部４０は、その具体的な構成を図１０に示すように、Ｋｅｍ発生モジュール４１、ＥＫｄ復号回路４３、ＥＫｓ復号回路４５やコンテンツデータ復号回路４６等からなる。

【００８２】

上記Ｋｅｍ発生モジュール４１は、著作権のライセンスを受ける際に与えられる秘密鍵であるマスターキーＫｍを記憶したＫｍメモリ４１Ａと、上記Ｋｍメモリ４１Ａにより与えられるマスターキーＫｍと上記認証処理部２６により与えられる認証済みの媒体識別情報DiscIDから上述の（１）式に示した演算処理によりイフェクティブマスターキーＫｅｍを生成するハッシュ関数回路４１Ｂとからなる。上記ハッシュ関数回路４１Ｂは、上記マスターキーＫｍと認証済みの媒体識別情報DiscIDから生成したイフェクティブマスターキーＫｅｍをＥＫｄ復号回路４３に供給する。

【００８３】

なお、このＫｅｍ発生モジュール４１は、上述の暗号化処理部３０のＫｅｍ発生モジュール３１と同じ構成のものであり、上記Ｋｅｍ発生モジュール３１を兼用するようにしてよい。

【００８４】

上記ＥＫｄ復号回路４３は、上記光ディスク１のリードインエリアから上記記録／再生ヘッド２３により再生される暗号化ディスクキーＥＫｄを上記イフェクティブマスターキーＫｍで復号してディスクキーＫｄを生成し、復号したディスクキーＫｄをＥＫｓ復号回路４５に供給する。

【００８５】

また、上記ＥＫｓ復号回路４５は、上記光ディスク１のデータエリアから上記記録／再生ヘッド２３により再生される暗号化セクタキーＥＫｓを上記ディスク

キーＫｄで復号してセクタキーＫｓを生成し、復号したセクタキーＫｓをコンテンツデータ復号回路４６に供給する。

【００８６】

上記コンテンツデータ復号回路４６は、上記光ディスク１のデータエリアから上記記録／再生ヘッド２３により再生される暗号化コンテンツデータを上記セクタキーＫｓで復号する。

【００８７】

このような構成の光ディスク記録／再生装置２０では、上記入力操作部２８から記録命令が入力されることにより制御部２９に記録モードが設定されると、上記制御部２９は、図１１のフローチャートに示すような手順でユーザデータを光ディスク１に記録するように、上記記録／再生部２７を制御する。

【００８８】

なお、以下の説明では、上記認証処理部２６により光ディスク１に対して既に認証処理が行われており、正当なものであると認証された光ディスク１に対してユーザデータを記録するものとする。

【００８９】

記録モードでは、上記記録／再生部２７の暗号化処理部３０が動作状態となっており、上記暗号化処理部３０のＫｅｍ発生モジュール３１は、上記認証処理部２６から認証済みの媒体識別情報DiscIDを受け取り（ステップＳ３１）、マスターキーＫｍをＫｍメモリ３１Ａから読み出して（ステップＳ３２）、ハッシュ関数回路３１Ｂにより上記媒体識別情報DiscIDとマスターキーＫｍからイフェクティブマスターキーＫｅｍを生成する（ステップＳ３３）。

【００９０】

次に、上記Ｋｄ暗号化／復号回路３３は、上記光ディスク１のリードインエリアに暗号化ディスクキーＥＫｄが記録されているか否かを判定する（ステップＳ３４）。

【００９１】

そして、上記Ｋｄ暗号化回路３３は、暗号化ディスクキーＥＫｄが記録されていない場合には、乱数発生回路３２により発生される例えば４０ビットの乱数を

ディスクキーＫｄとし（ステップＳ３５）、このディスクキーＫｄを上記イフェクティブマスターキーＫｅｍで暗号化して暗号化ディスクキーＥＫｄを生成し、この暗号化ディスクキーＥＫｄを上記光ディスク１のリードインエリアに記録する（ステップＳ３６）。

【００９２】

また、上記Ｋｄ暗号化回路３３は、暗号化ディスクキーＥＫｄが記録されていた場合には、上記暗号化ディスクキーＥＫｄを上記イフェクティブマスターキーＫｍで復号して、ディスクキーＫｄを得る（ステップＳ３７）。

【００９３】

次に、上記Ｋｓ暗号化回路３５は、上記乱数発生回路３２により発生される４０ビットの乱数をセクタキーＫｓｉとし（ステップＳ３８）、このセクタキーＫｓｉを上記ディスクキーＫｄで暗号化して暗号化セクタキーＥＫｓｉを生成し、この暗号化セクタキーＥＫｓｉをセクタヘッダに記録する（ステップＳ３９）。

【００９４】

そして、上記コンテンツデータ暗号化回路３６は、ユーザデータを上記セクタキーＫｓｉで暗号化して暗号化コンテンツデータを生成し、この暗号化コンテンツデータは、メインデータ部に記録する（ステップＳ４０）。

【００９５】

さらに、上記コンテンツデータ暗号化回路３６は、記録すべきユーザデータをすべて記録したか否かを判定し（ステップＳ４１）、記録すべきユーザデータがある場合には、次のセクタにアクセスし（ステップＳ４２）、上記ステップＳ３８に戻って、上記ステップＳ３８からステップＳ４２の処理を繰り返し行う。

【００９６】

このようにしてユーザデータをすべて上記光ディスク１のデータエリアに記録し終えたら、記録モードを終了する。

【００９７】

また、この光ディスク記録／再生装置２０では、上記入力操作部２８から記録命令が入力されることにより制御部２９に再生モードが設定されると、上記制御部２９は、図１２のフローチャートに示すような手順で光ディスク１からユーザ

データを再生するするように、上記記録／再生部２７を制御する。

【００９８】

なお、以下の説明では、上記認証処理部２６により光ディスク１に対して既に認証処理が行われており、正当なものであると認証された光ディスク１からユーザデータを再生するものとする。

【００９９】

再生モードでは、上記記録／再生部２７の復号処理部４００が動作状態となっており、上記復号処理部４０のＫｅｍ発生モジュール４１は、上記認証処理部２６から認証済みの媒体識別情報DiscIDを受け取り（ステップＳ５１）、マスターキーＫｍをＫｍメモリ４１Ａから読み出して（ステップＳ５２）、ハッシュ関数回路４１Ｂにより上記媒体識別情報DiscIDとマスターキーＫｍからイフェクティブマスターキーＫｅｍを生成する（ステップＳ５３）。

【０１００】

次に、上記ＥＫｄ暗号化／復号回路３３は、上記光ディスク１のリードインエリアから再生される暗号化ディスクキーＥＫｄを上記イフェクティブマスターキーＫｅｍで復号して、ディスクキーＫｄを生成する（ステップＳ５４）。

【０１０１】

次に、上記ＥＫｓ復号回路３５は、上記光ディスク１のデータエリアから再生される暗号化セクタキーＥＫｓｉを復号して、セクタキーＫｓｉを生成する（ステップＳ５５）。

【０１０２】

そして、上記コンテンツデータ復号回路４６は、上記光ディスク１のデータエリアから再生される暗号化コンテンツデータを上記セクタキーＫｓで復号する（ステップＳ５６）。

【０１０３】

さらに、上記コンテンツデータ復号回路４６は、再生すべきコンテンツデータをすべて再生したか否かを判定し（ステップＳ５７）、再生すべきコンテンツデータがある場合には、次のセクタにアクセスし（ステップＳ５８）、上記ステップＳ２５に戻って、上記ステップＳ５５からステップＳ５８の処理を繰り返し行

う。

【０１０４】

このようにして必要なコンテンツデータをすべて上記光ディスク１のデータエリアに再生し終えたら、再生モードを終了する。

【０１０５】

この光ディスク記録／再生装置２０によりユーザデータ記録部３にユーザデータが記録された光ディスク１は、上記ユーザデータの暗号鍵すなわちセクタキーＫｓが上記ディスクキーＫｄで暗号化した暗号化セクタキーＥＫｓとしてデータエリアに記録され、さらに、上記ディスクキーＫｄが、この光ディスク１に固有の媒体識別情報DiscＩＤに基づいて生成されたイフェクティブマスターキーＫｅｍで暗号化した暗号化ディスクキーＥＫｄとしてリードインエリアに記録されているので、上記光ディスク１のランダムパターン情報記録部４に記録されているランダムパターン情報に基づいて生成される媒体識別情報検査データと認証データ記録部５に記録された認証データに基づいて上記媒体識別情報DiscＩＤについて認証処理を行う認証処理機能を有する正規の再生装置でのみ再生することができ、上記認証処理機能にない再生装置ではユーザデータを復号して再生することはできない。

【０１０６】

また、仮に、上記光ディスク１のデータエリア及びリードインエリアのデータをそのまま新しいディスクに不正コピーされた場合としても、上記光ディスク１のランダムパターン情報記録部４に記録されているランダムパターン情報はランダムな物理現象によるものであるから、上記新しいディスクがランダムパターン情報記録部を有する正規のものであったとしても、新しいディスクのランダムパターン情報記録部から上記光ディスク１のランダムパターン情報記録部４に記録されているランダムパターン情報と同じランダムパターン情報を検出することはできない。したがって、不正コピーされたディスクが正規の再生装置により再生されることはない。

【０１０７】

ここで、上述の光ディスク記録／再生装置２０では、暗号化処理処理部３０に

おいて、上記認証処理部２６により認証された光ディスク１の媒体識別情報DiscＩＤに基づいて、マスターキーＫｍからイフェクティブマスターキーＫｅｍを生成し、このイフェクティブマスターキーＫｅｍでディスクキーＫｄを暗号化し、上記ユーザデータの暗号化に用いる暗号鍵すなわちセクターキーＫｓを上記ディスクキーＫｄで暗号化し、上記セクターキーＫｓにより暗号化したユーザデータと上記暗号化したディスクキーＫｄ及びセクターキーＫｓを上記光ディスク１に記録するようにしたが、上記認証処理部２６により認証された光ディスク１の媒体識別情報DiscＩＤに基づいて、上記ユーザデータを暗号化するようにしてもよい。例えば、例えば図１３に示すように、上記乱数発生回路３２で乱数として発生されるセクターキーＫｓから上記イフェクティブマスターキーＫｅｍに基づいてイフェクティブセクターＫｅｓを生成するセクターキー生成部１３０を設け、上記コンテンツデータ暗号化回路３５において、上記セクターキー生成回路１３０により生成されたイフェクティブセクターキーＫｅｓでユーザデータを暗号化して暗号化コンテンツデータを生成する。

【０１０８】

この場合、復号処理部４０には、図１４に示すように、イフェクティブマスターキーＫｅｍに基づいてセクタキーＫｓからイフェクティブセクターキーＫｅｓを生成するＫｅｓ生成回路１４０を設け、上記光ディスク１のデータエリアから上記記録／再生ヘッド２３により再生される暗号化セクタキーＥＫｓを上記ＥＫｓ復号回路４５により上記ディスクキーＫｄで復号してセクターキーＫｓを生成し、このセクターキーＫｓから上記Ｋｅｓ生成回路１４０によりイフェクティブセクタキーＫｅｓを生成して、このイフェクティブセクタキーＫｅｓを用いてコンテンツデータ復号回路４６により暗号化コンテンツデータを復号する。

【０１０９】

また、上述の実施の形態では、図１に示すような構成の光ディスク１を用いた記録／再生システムに本発明を適用したが、図１５に示すようなカード状記録媒体５１を用いた記録／再生システムを構築するようにしてもよい。

【０１１０】

すなわち、この図１３に示したカード状記録媒体５１は、ユーザデータが記録

されるユーザデータ記録部５３と、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部５４と、上記ランダムパターン情報記録部５４から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部５５とを有する。

【０１１１】

このような構成のカード状記録媒体５１を使用する記録／再生システムでは、上述の光ディスク記録／再生システムと同様に、上記ランダムパターン情報記録部５４からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成するとともに、上記情報記録媒体上の認証データ記録部５５から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報と上記認証データに基づいて上記情報記録媒体に対する認証処理を行うことができ、上記認証処理により認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化したデータを上記認証された情報記録媒体上のユーザデータ記録部５３を介して記録／再生することにより、上記ユーザデータ記録部５３の情報の不正コピーを確実に防止することが可能となる。

【０１１２】

【発明の効果】

以上詳細に説明したように、本発明によれば、情報記録媒体上にランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部を設けた情報記録媒体の上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成して、上記媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして上記情報記録媒体上の認証データ記録部に記録することによって、媒体識別情報を該媒体識別情報に対する製造者毎のデジタル署名とともに認証データとして認証データ記録部に記録した情報記録媒体を提供することができる。そして、ランダムな物理現象によるランダムパターン情報を記録したランダムパターン情報記録部と、上記ランダムパターン情報記録部から検出

されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名を認証データとして格納した認証データ記録部と、ユーザデータが記録されるユーザデータ記録部とを有する情報記録媒体に対して、上記ランダムパターン情報記録部からランダムな物理現象によるランダムパターン情報を検出し、該ランダムパターン情報から媒体識別情報を生成するとともに、上記情報記録媒体上の認証データ記録部から認証データを再生し、上記ランダムパターン情報から生成した媒体識別情報と上記認証データに基づいて上記情報記録媒体に対する認証処理を行うことができ、上記認証処理により認証された情報記録媒体の媒体識別情報から暗号鍵を生成し、上記暗号鍵を用いてデータを暗号化したデータを上記認証された情報記録媒体上のユーザデータ記録部を介して記録／再生することにより、ＲＡＭメディアに対しても有効な不正コピー防止システムを構築することができる。

【図面の簡単な説明】

【図１】

本発明を適用した光ディスクを説明するための図である。

【図２】

上記光ディスクに認証データを記録する認証データ記録装置の構成を示すブロック図である。

【図３】

上記認証データ記録装置における認証データ生成部の具体的な処理内容を示すフローチャートである。

【図４】

上記光ディスクを使用する光ディスク記録／再生装置の構成を示すブロック図である。

【図５】

上記光ディスク記録／再生装置における認証処理部の具体的な処理内容を示すフローチャートである。

【図６】

上記認証処理部による認証処理に使用されるリボケーションリストを示す図で

ある。

【図７】

上記認証処理部による認証処理に使用される公開鍵リストを示す図である。

【図８】

上記光ディスク記録／再生装置における記録／再生回路の暗号化処理部の構成を示すブロック図である。

【図９】

上記光ディスク記録／再生装置により光ディスクに記録されるデータの構造を模式的に示す図である。

【図１０】

上記光ディスク記録／再生装置における記録／再生回路の復号処理部の構成を示すブロック図である。

【図１１】

上記光ディスク記録／再生装置の記録モードの動作を示すフローチャートである。

【図１２】

上記光ディスク記録／再生装置の再生モードの動作を示すフローチャートである。

【図１３】

上記光ディスク記録／再生装置における記録／再生回路の暗号化処理部の他の構成例を示すブロック図である。

【図１４】

上記光ディスク記録／再生装置における記録／再生回路の復号処理部の他の構成例を示すブロック図である。

【図１５】

本発明を適用したカード状情報記録媒体を説明するための図である。

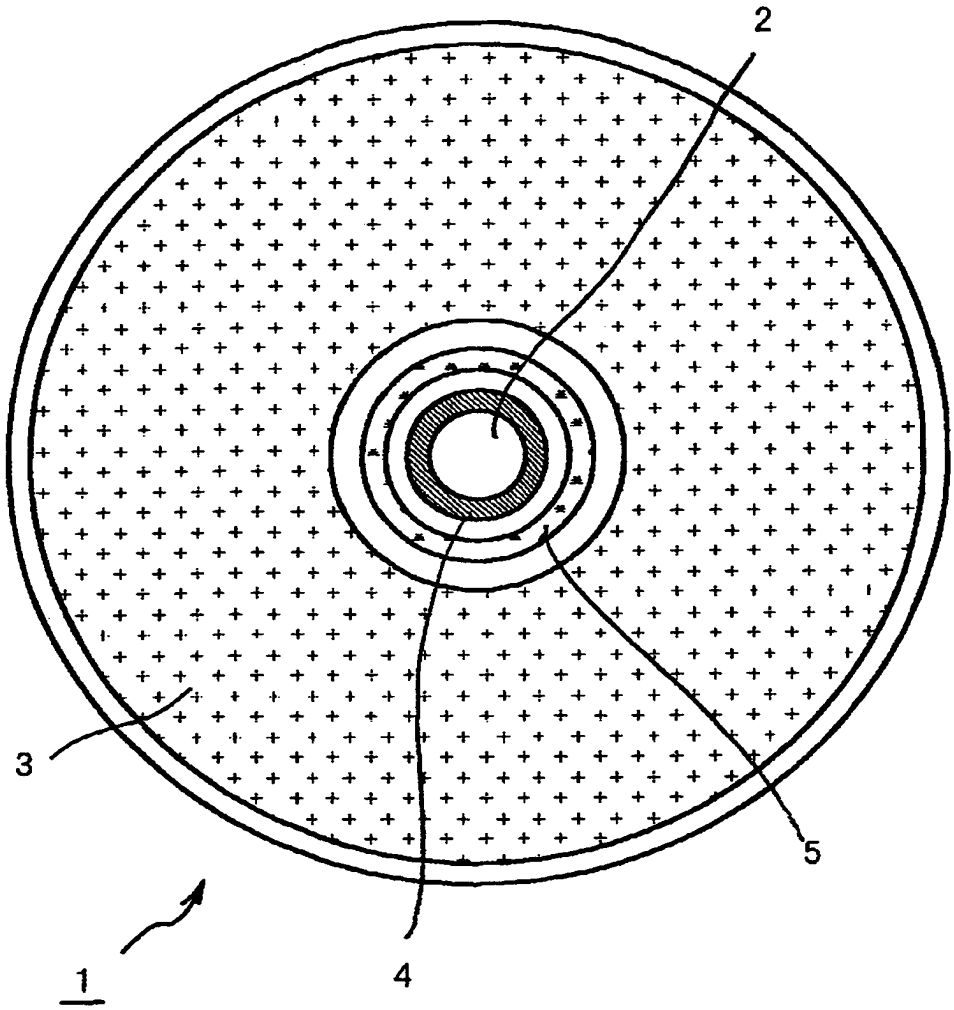
【符号の説明】

１　光ディスク、３，５３　ユーザデータ記録部、４，５４　ランダムパター情報記録部、５，５５　認証データ記録部、１０　認証データ記録装置、１３

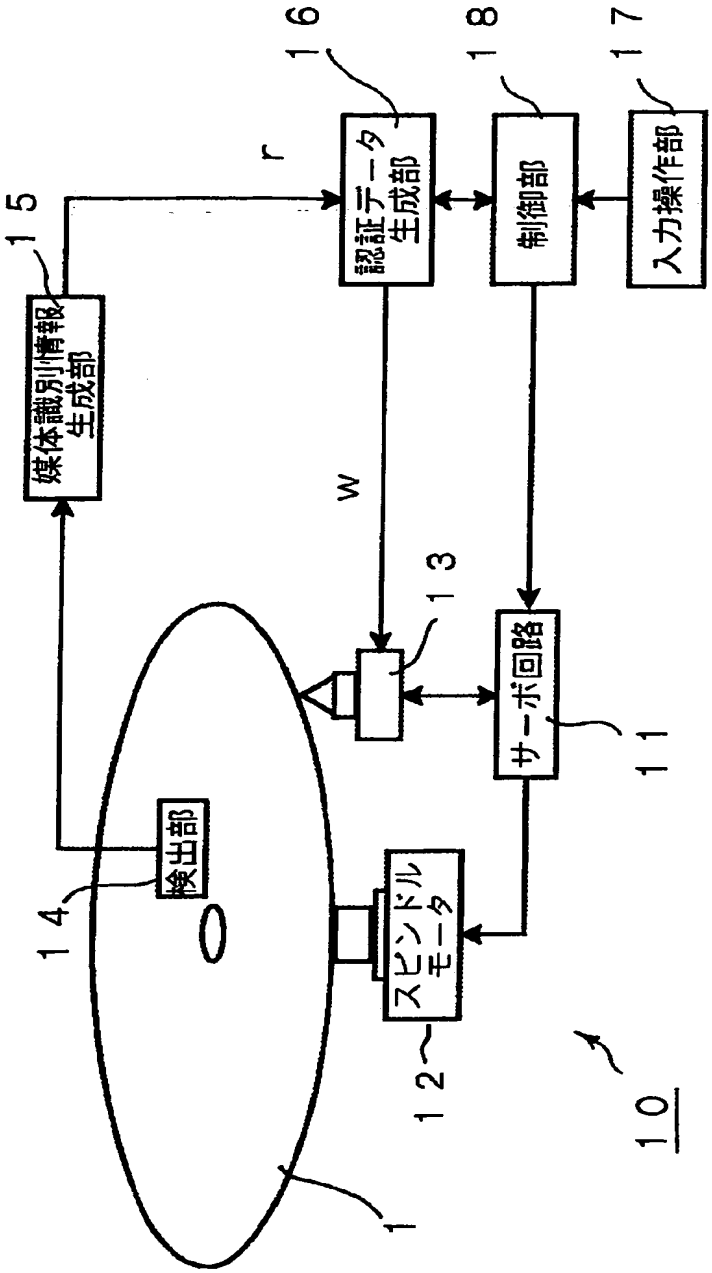
，２３　記録／再生ヘッド、１４，２４　ランダムパターン情報検出部、１５，２５　媒体識別情報生成部、１６　認証データ生成部、２０　光ディスク記録／再生装置、３０　暗号化処理部、４０復号処理部、１３０、１４０　Ｋｅｓ生成回路

【書類名】　図面

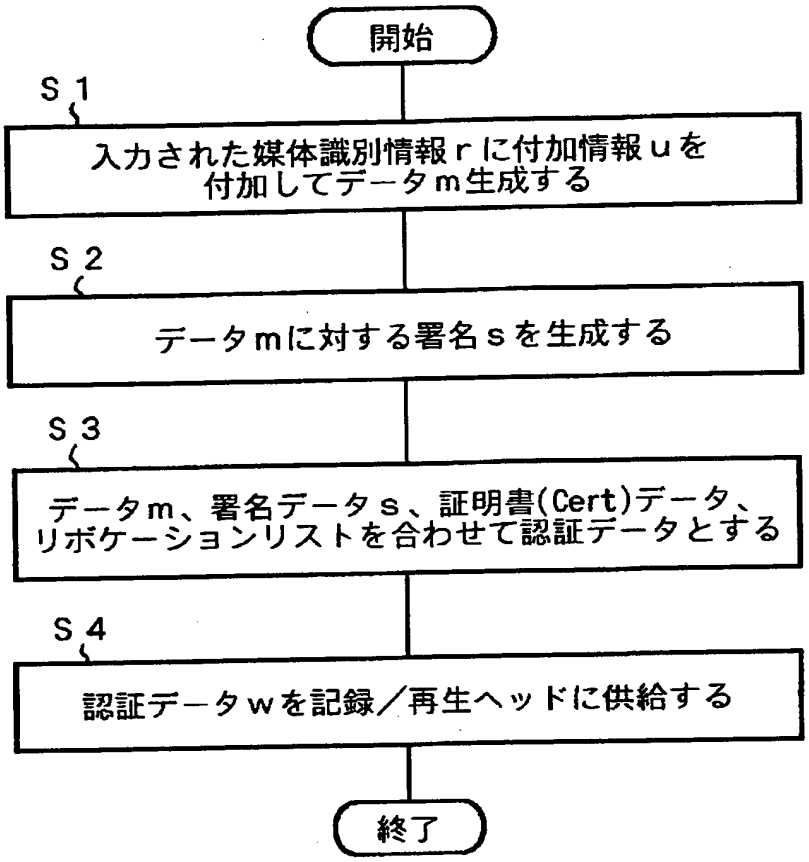
【図１】



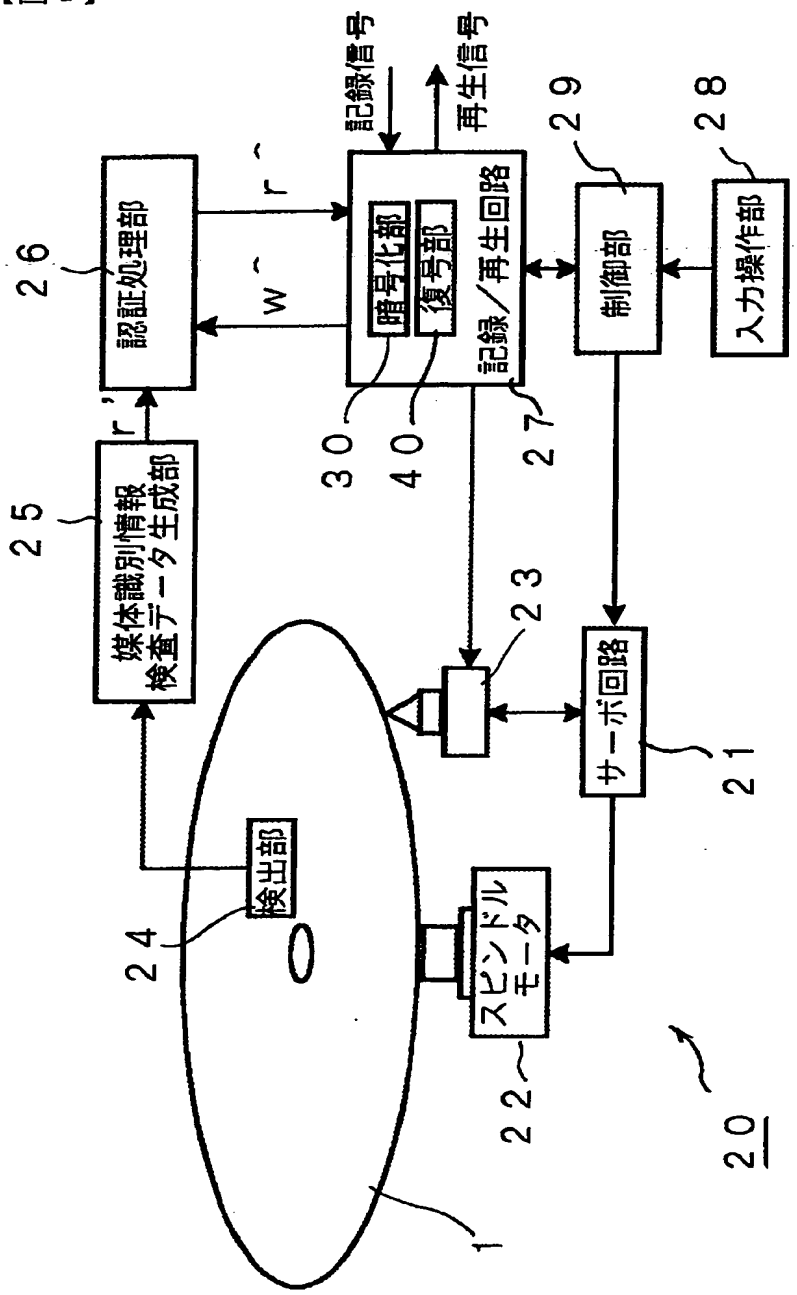
【図２】


16
18
17
r
15
認証データ生成部
制御部
入力操作部
媒体識別情報生成部
W
13
サーボ回路
11
検出部
14
スピンドルモータ
12
10
1

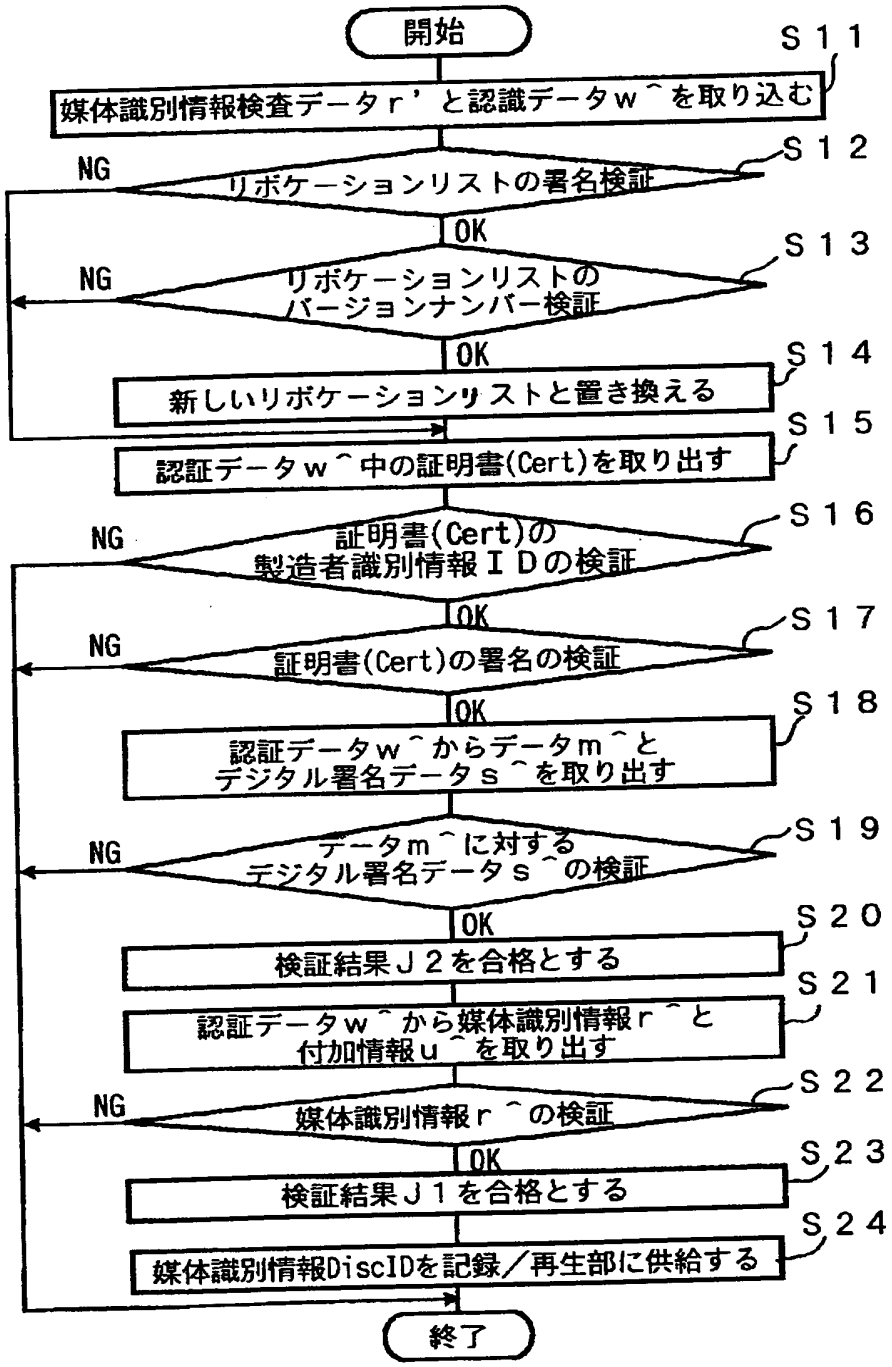
【図３】


開始
S 1
入力された媒体識別情報ｒに付加情報ｕを
付加してデータｍ生成する
S 2
データｍに対する署名ｓを生成する
S 3
データｍ、署名データｓ、証明書(Cert)データ、
リボケーションリストを合わせて認証データとする
S 4
認証データｗを記録／再生ヘッドに供給する
終了

【図４】


記録信号
再生信号
29
28
26
r
w
暗号化部
復号部
記録／再生回路
制御部
入力操作部
30
40
27
r'
25
媒体識別情報
検査データ生成部
23
サーボ回路
21
検出部
24
スピンドル
モータ
22
20
1

【図５】


開始
S11
媒体識別情報検査データｒ'と認識データｗ^を取り込む
S12
NG
リボケーションリストの署名検証
OK
S13
NG
リボケーションリストの
バージョンナンバー検証
OK
S14
新しいリボケーションリストと置き換える
S15
認証データｗ^中の証明書(Cert)を取り出す
S16
NG
証明書(Cert)の
製造者識別情報ＩＤの検証
OK
S17
NG
証明書(Cert)の署名の検証
OK
S18
認証データｗ^からデータｍ^と
デジタル署名データｓ^を取り出す
S19
NG
データｍ^に対する
デジタル署名データｓ^の検証
OK
S20
検証結果Ｊ２を合格とする
S21
認証データｗ^から媒体識別情報ｒ^と
付加情報ｕ^を取り出す
S22
NG
媒体識別情報ｒ^の検証
OK
S23
検証結果Ｊ１を合格とする
S24
媒体識別情報DiscIDを記録／再生部に供給する
終了

【図６】

リボケーションリスト

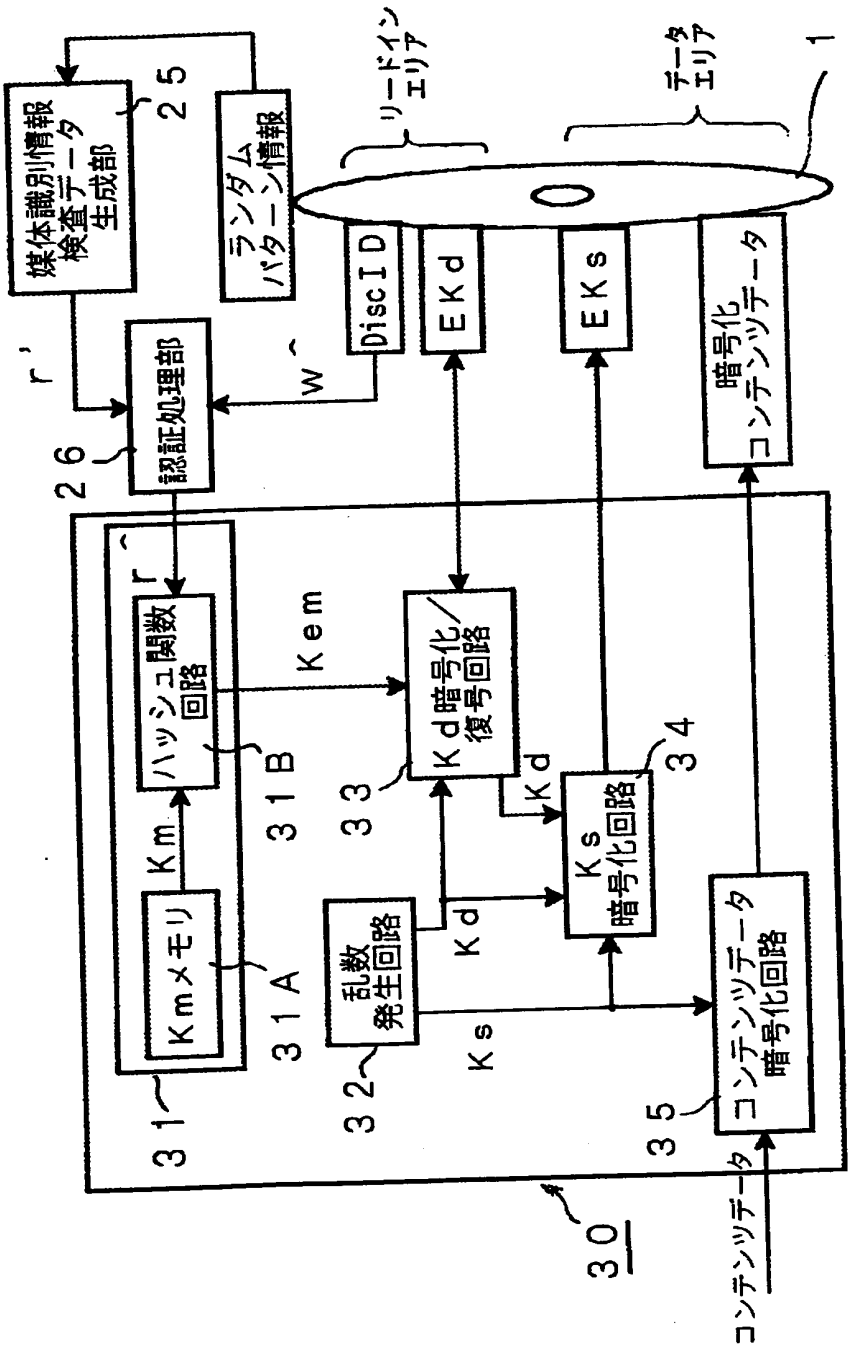
| バージョンナンバー |
|---|
| 製造者ＩＤ |
| ・・・ |
| |
| |

【図７】

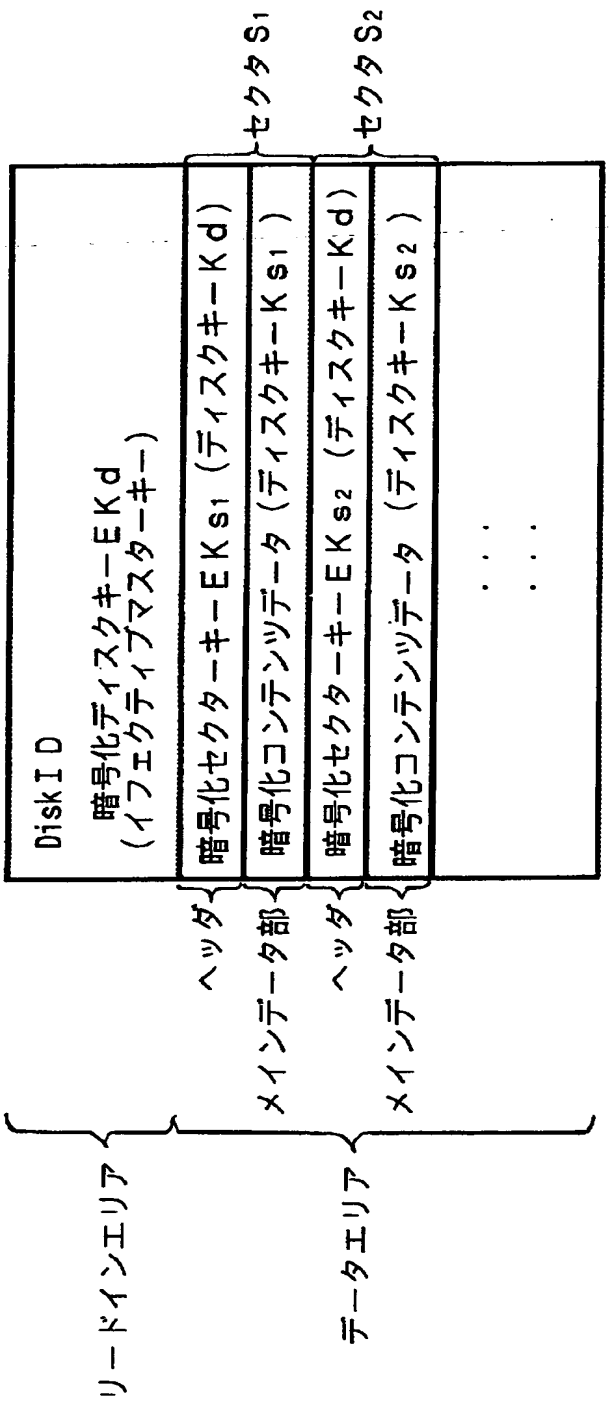
公開鍵リスト

| 最新のリボケーションリストのバージョンナンバー | | |
|---|---|---|
| 製造者ＩＤ | 公開鍵 | リボケーションフラグ(YES/NO) |
| ・・・ | ・・・ | ・・・ |
| | | |
| | | |

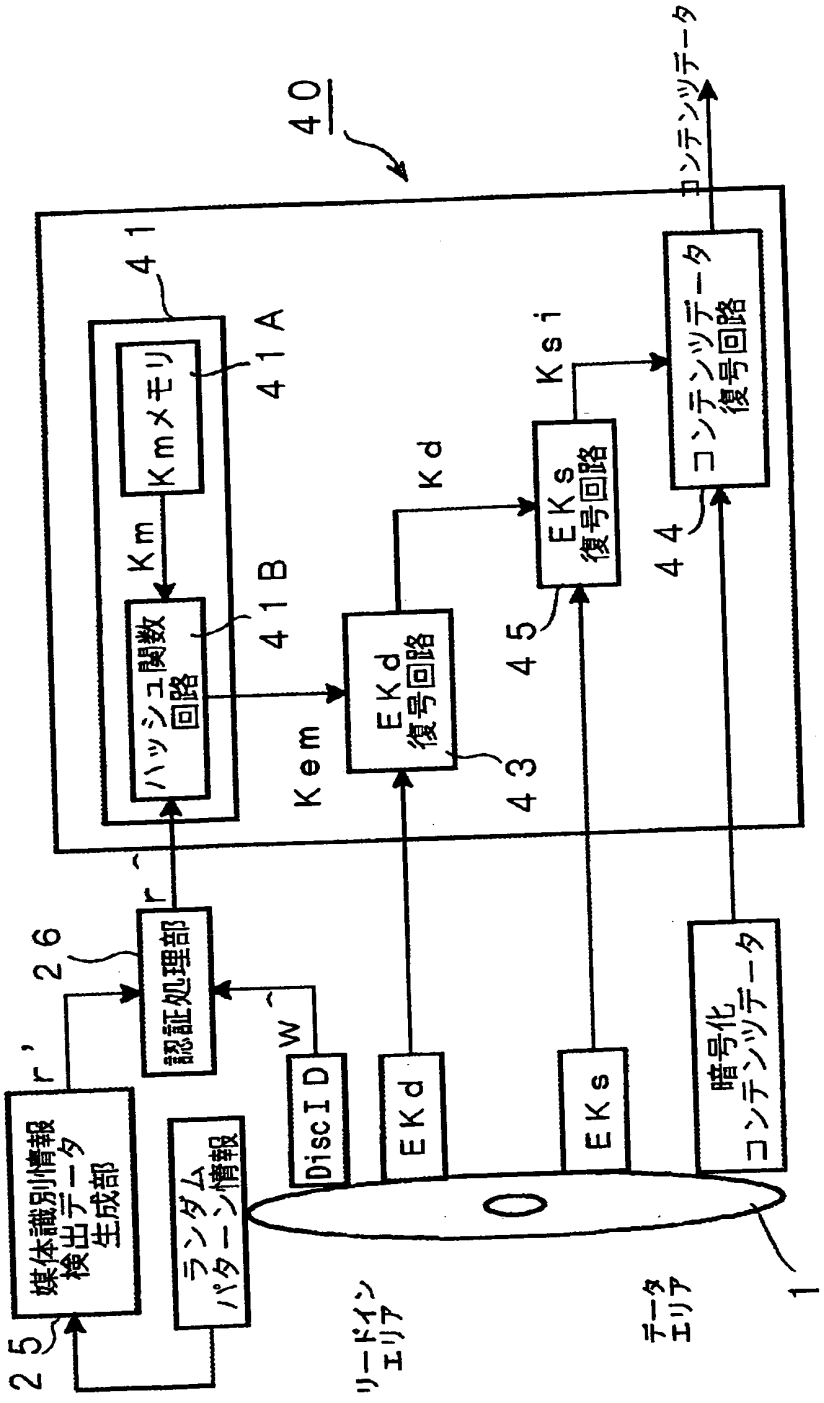
【図８】


媒体識別情報検査データ生成部
25
ランダムパターン情報
リードインエリア
データエリア
1
DiscID
EKd
EKs
暗号化コンテンツデータ
r'
r^
W^
26
認証処理部
ハッシュ関数回路
Kem
Kd暗号化／復号回路
Kd
Ks暗号化回路
34
Km
Kmメモリ
31B
33
31A
乱数発生回路
Kd
Ks
32
31
35
コンテンツデータ暗号化回路
30
コンテンツデータ

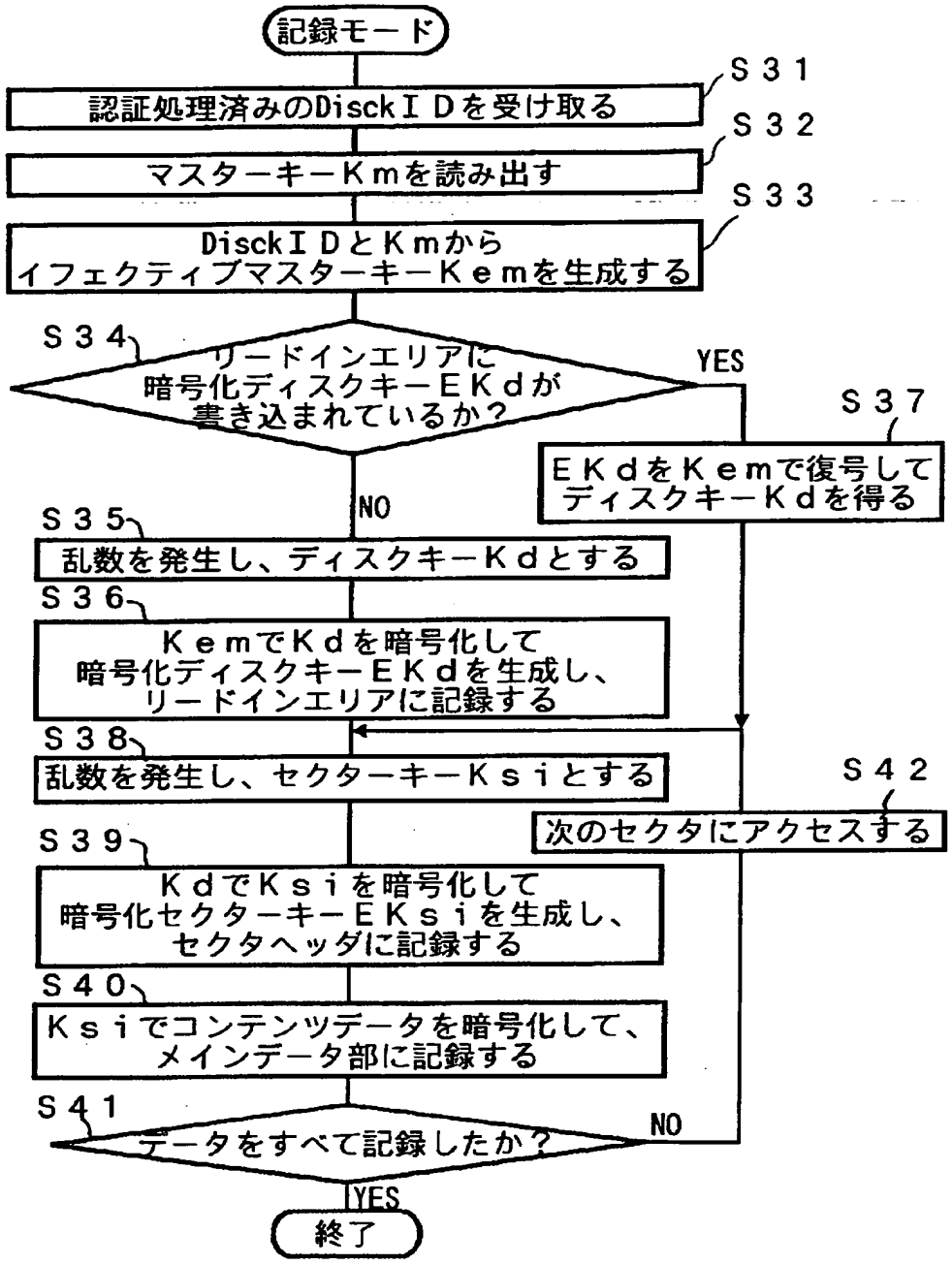
【図９】


セクタS1
セクタS2
DiskID
暗号化ディスクキーEKd
（イフェクティブマスターキー）
暗号化セクターキーEKs1（ディスクキーKd）
暗号化コンテンツデータ（ディスクキーKs1）
暗号化セクターキーEKs2（ディスクキーKd）
暗号化コンテンツデータ（ディスクキーKs2）
ヘッダ
メインデータ部
ヘッダ
メインデータ部
リードインエリア
データエリア

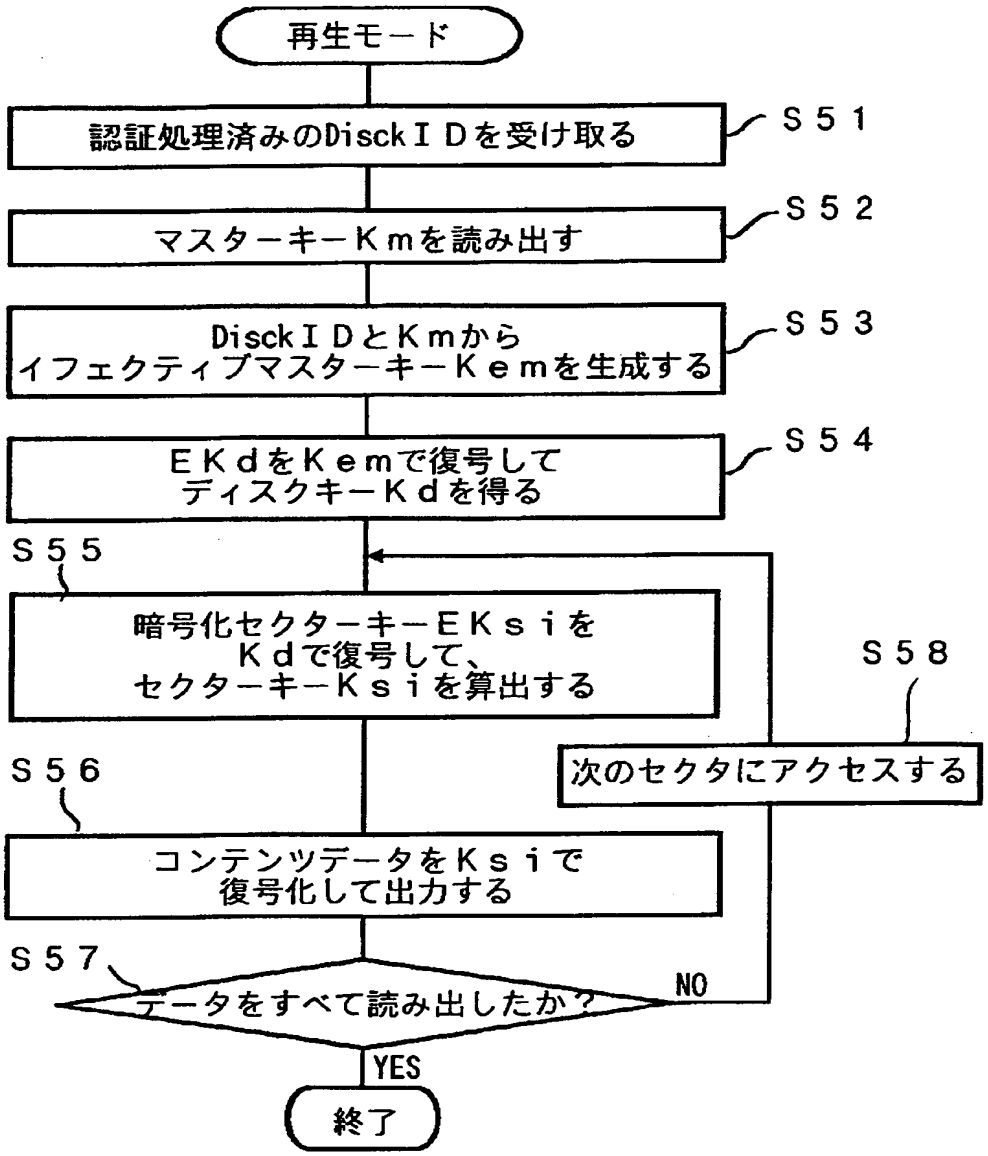
【図１０】


40
41
41A
Kmメモリ
Km
41B
ハッシュ関数回路
Kem
EKd復号回路
43
Kd
45
EKs復号回路
Ksi
44
コンテンツデータ復号回路
コンテンツデータ
r
26
認証処理部
r'
W
媒体識別情報検出データ生成部
ランダムパターン情報
DiscID
EKd
EKs
暗号化コンテンツデータ
25
リードインエリア
データエリア
1

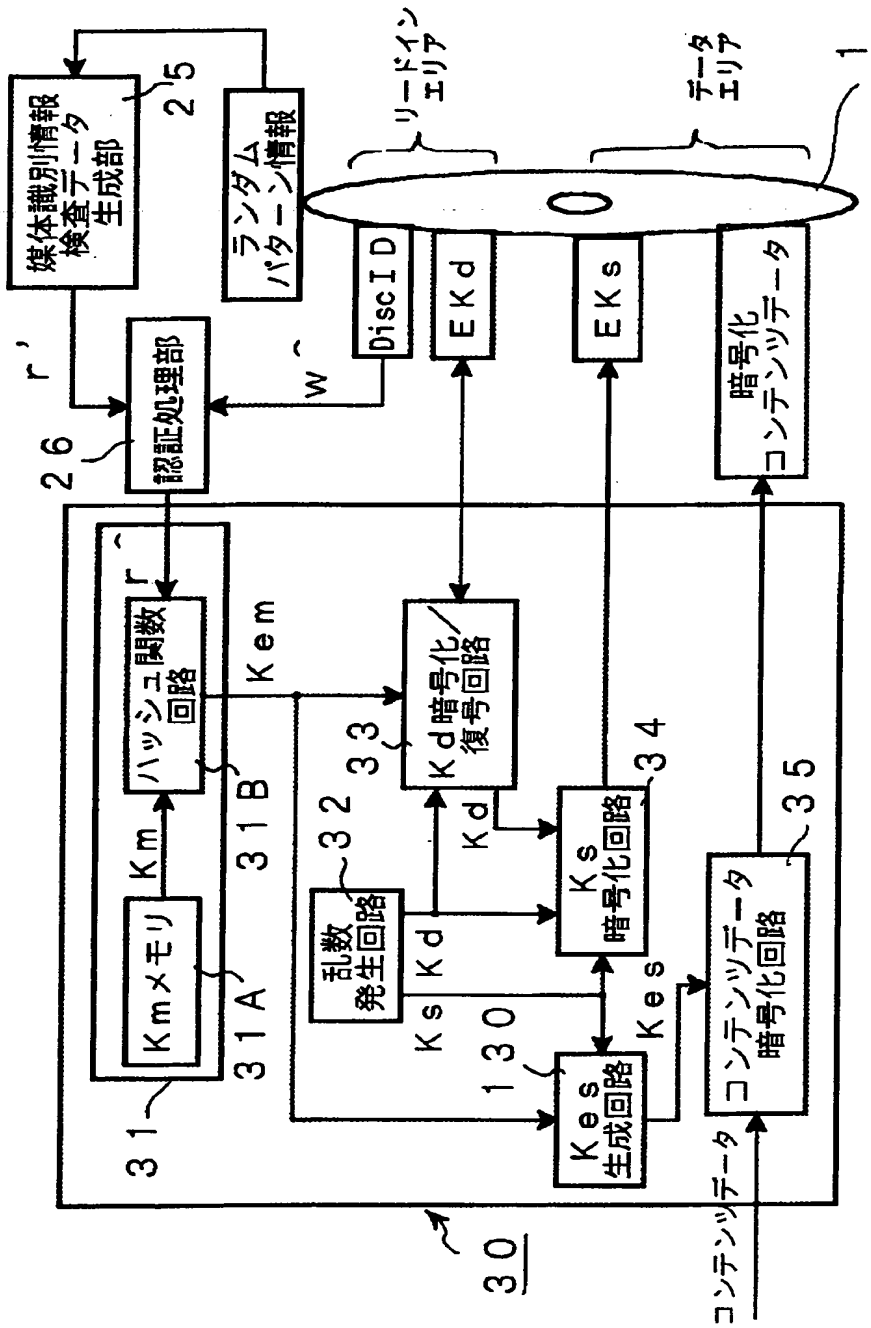
【図１１】


記録モード
S31
認証処理済みのDisckＩＤを受け取る
S32
マスターキーＫｍを読み出す
S33
DisckＩＤとＫｍから
イフェクティブマスターキーＫｅｍを生成する
S34
リードインエリアに
暗号化ディスクキーＥＫｄが
書き込まれているか？
YES
NO
S35
乱数を発生し、ディスクキーＫｄとする
S36
ＫｅｍでＫｄを暗号化して
暗号化ディスクキーＥＫｄを生成し、
リードインエリアに記録する
S37
ＥＫｄをＫｅｍで復号して
ディスクキーＫｄを得る
S38
乱数を発生し、セクターキーＫｓｉとする
S39
ＫｄでＫｓｉを暗号化して
暗号化セクターキーＥＫｓｉを生成し、
セクタヘッダに記録する
S40
Ｋｓｉでコンテンツデータを暗号化して、
メインデータ部に記録する
S41
データをすべて記録したか？
NO
YES
終了
S42
次のセクタにアクセスする

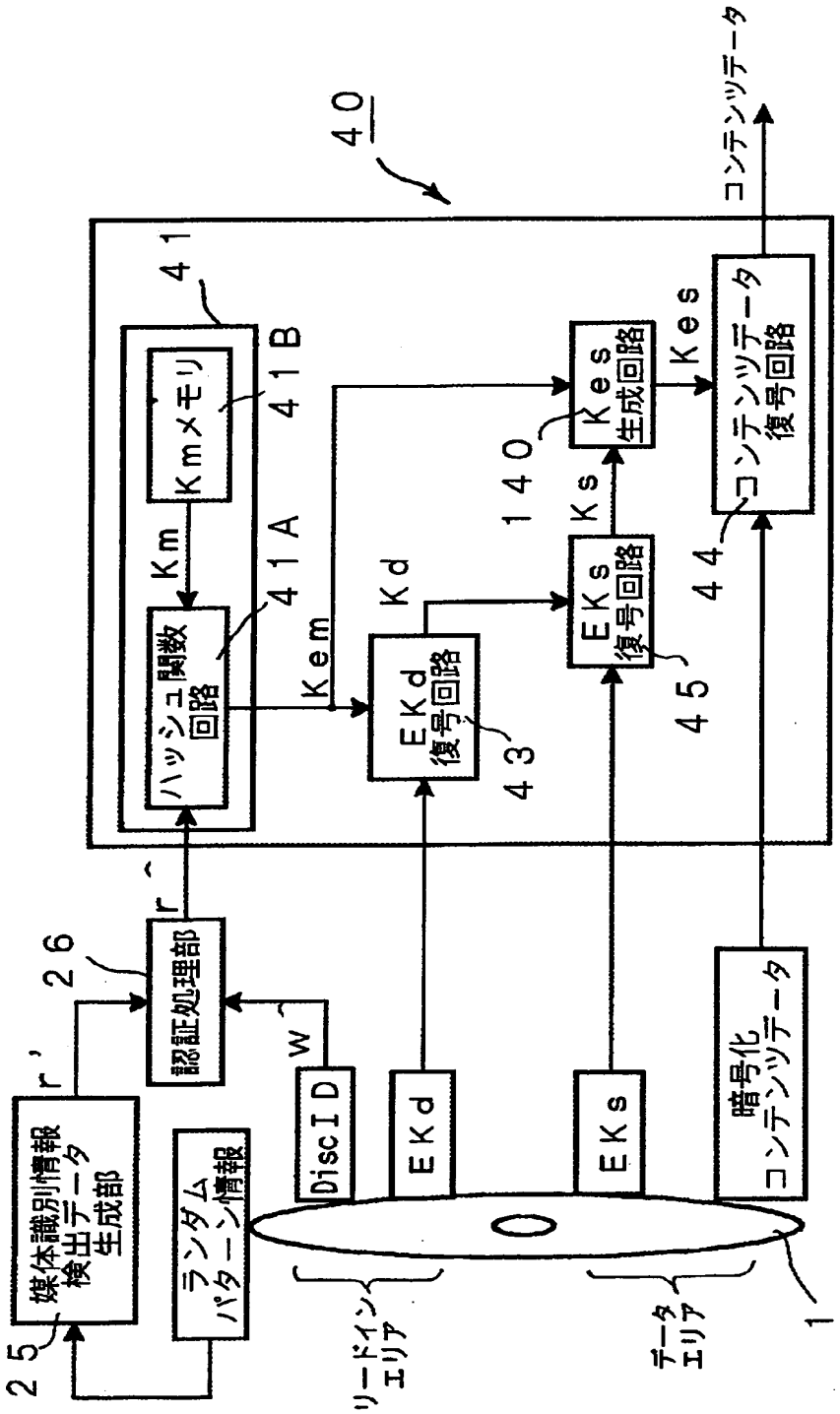
【図１２】


再生モード
認証処理済みのDisckＩＤを受け取る
Ｓ５１
マスターキーＫｍを読み出す
Ｓ５２
DisckＩＤとＫｍから
イフェクティブマスターキーＫｅｍを生成する
Ｓ５３
ＥＫｄをＫｅｍで復号して
ディスクキーＫｄを得る
Ｓ５４
Ｓ５５
暗号化セクターキーＥＫｓｉを
Ｋｄで復号して、
セクターキーＫｓｉを算出する
Ｓ５８
次のセクタにアクセスする
Ｓ５６
コンテンツデータをＫｓｉで
復号化して出力する
Ｓ５７
データをすべて読み出したか？
NO
YES
終了

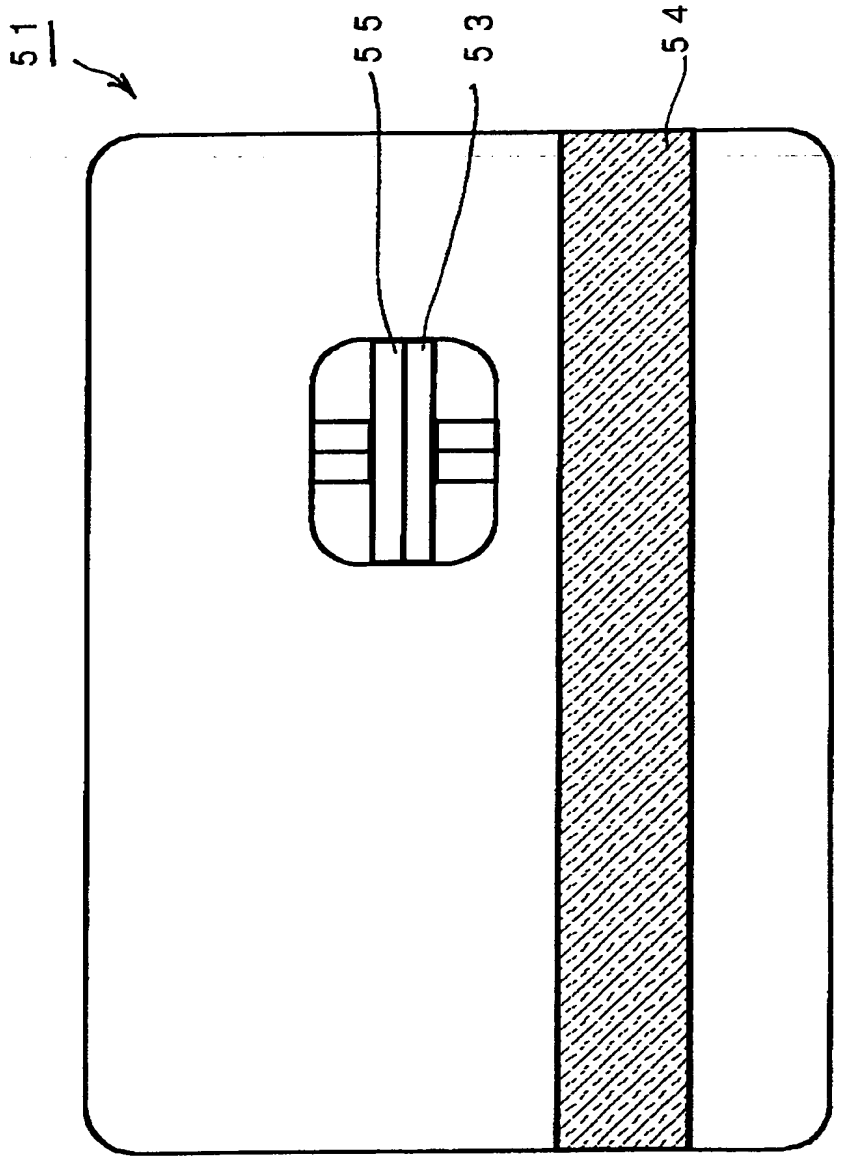
【図１３】


媒体識別情報検査データ生成部
25
ランダムパターン情報
リードインエリア
データエリア
1
DiscID
EKd
EKs
暗号化コンテンツデータ
認証処理部
26
r'
W
r
ハッシュ関数回路
Kem
Kd暗号化/復号回路
33
31B
32
34
35
Km
Kmメモリ
31A
乱数発生回路
Kd
Ks暗号化回路
Ks
Kes
130
Kes生成回路
コンテンツデータ暗号化回路
31
30
コンテンツデータ

【図１４】


40
41
41B
Kmメモリ
Km
41A
ハッシュ関数回路
Kem
Kd
EKd復号回路
43
140
Ks
EKs復号回路
45
Kes
Kes生成回路
44
コンテンツデータ復号回路
コンテンツデータ
r
26
認証処理部
r'
W
媒体識別情報検出データ生成部
ランダムパターン情報
DiscID
EKd
EKs
暗号化コンテンツデータ
25
リードインエリア
データエリア
1

【図１５】



【書類名】　　要約書

【要約】

【課題】　ＲＡＭメディアに対しても有効な不正コピー防止システムを構築する。

【解決手段】　情報記録媒体上に、ユーザデータが記録されるユーザデータ記録部３と、ランダムな物理現象によるランダムパターン情報が記録されたランダムパターン情報記録部４と、上記ランダムパターン情報記録部４から検出されるランダムパターン情報に基づいて生成された媒体識別情報と、上記媒体識別情報に対する製造者毎のデジタル署名が認証データとして記録された認証データ記録部５とを設ける。

【選択図】　　図１

# 出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社